

Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT)

Justo Carracedo Gallardo,¹ Ana Gómez Oliva²,
Jesús Moreno Blázquez³, Emilia Pérez Belleboni⁴
Departamento de Ingeniería y Arquitecturas Telemáticas.
Universidad Politécnica de Madrid
Ctra. Valencia km. 7. 28031 Madrid.
Teléfono: 913 367 817. Fax: 913 367 817
{carracedo¹, agomez², jmoreno³, belleboni⁴}@diatel.upm.es

José David Carracedo Verde
Departamento de Ciencia Política y de la
Administración III. Universidad Complutense de
Madrid
Campus de Somosaguas. 28223 Madrid
Teléfono: 913 942 664. Fax: 913 942 776
jdcarcedo@proyectos.diatel.upm.es

Resumen

Esta ponencia presenta un visión global de un esquema de voto electrónico desarrollado dentro del proyecto VOTESCRIPT, auspiciado por el ministerio español de Ciencia y Tecnología (TIC2000-1630-C02). En primer lugar se realiza una tipificación de los sistemas que pueden considerarse de votación electrónica, para analizar, a continuación, los sistemas más relevantes que se apoyan en criptografía avanzada y redes telemáticas. Se comenta el proceso de investigación multidisciplinar seguido para la determinación de los requisitos que debe cumplir el sistema de votación y se describe, de forma somera, las principales características del sistema desarrollado y su comportamiento global.

1. Introducción

La explosión actual del uso de Internet, tanto en España como en el resto del mundo, supone un reto para las políticas democráticas: usar las nuevas tecnologías para promover cambios sociales progresivos con objeto de crear una sociedad más democrática e igualitaria. En este sentido, la proliferación de los ordenadores y la conectividad universal ofrecida por Internet han preparado el camino para el desarrollo del voto electrónico en su concepción más avanzada, esto es, votación desde un ordenador personal ubicado en el domicilio particular o centro de trabajo.

En los últimos años, diversos gobiernos e instituciones han realizado algunos ensayos con sistemas de voto electrónico a través de Internet, detectándose que todavía existe una falta de madurez en el desarrollo de éstos a la que contribuyen diversos factores. El primero de ellos estriba en la dificultad técnica de satisfacer plenamente los rigurosos requisitos de seguridad que debe proporcionar un

sistema de votación para garantizar la corrección del proceso en todas sus fases (autenticación de los usuarios, votación y recuento). El segundo factor que impide el pleno desarrollo de estos sistemas surge de la necesidad de garantizar el derecho al voto para todos los ciudadanos, lo cual desde un punto de vista político supone un importante reto. Sin embargo, parece que la causa primordial de que estos sistemas de votación electrónica no estén siendo utilizados masivamente radica en el que cambio cultural que el nuevo sistema supondrá para los ciudadanos. En efecto, no sólo deberán desarrollar nuevas habilidades para poder utilizar el sistema, sino que habrán de confiar en sistemas informáticos, cuya tecnología conocen vagamente, pero de los que sospechan que son mucho más susceptibles a la manipulación que los sistemas tradicionales de votación. Los sistemas de voto electrónico que aspiren a sustituir algún día el sistema de voto tradicional deberán incorporar las bondades de estos, a la vez que deberán ofrecer nuevas facilidades que permitan contrarrestar la natural desconfianza de los votantes hacia el proceso de votación electrónica.

Este artículo se presenta como resultado parcial del proyecto *VOTESCRIPT: Votación Electrónica Segura basada en criptografía avanzada*, subvencionado dentro del Plan Nacional de I+D+I (código TIC 2000-1630), que tiene como objetivo final la modelización y desarrollo de un prototipo de sistema de votación electrónica para realizar votaciones seguras mediante el empleo de redes de ordenadores públicas y, a priori, no seguras. Dentro de este mismo contexto, se está realizando una colaboración con la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, que en la actualidad desarrolla para el Ministerio del Interior un proyecto de implantación de un sistema de

votación para los españoles residentes en el extranjero a través de Internet.

En el proyecto VOTESCRIPT se ha abordado la votación desde cabinas o kioscos de votación a los que los ciudadanos tienen acceso, posponiendo la votación desde casa, a través de Internet, a etapas posteriores de desarrollo. Las razones para esta postura no son exclusivamente de índole técnico, sino que como se ha comentado, es preciso que se produzca un proceso de maduración tanto tecnológico como político y social para que los nuevos sistemas sean mayoritariamente aceptados. Es de destacar, que las recomendaciones recogidas en el *Report of the National Workshop on Internet Voting* del Internet Policy Institute [1] (marzo 2001) y las conclusiones de la experiencia de Contra Costa [2] (California, noviembre 2000) se decantan en este sentido.

Para llevar a cabo el diseño global de la arquitectura del sistema, se ha trabajado en dos ámbitos distintos y complementarios: la seguridad de todo el sistema de votación y la eliminación de las barreras culturales que dificultasen la aceptación del mismo por los ciudadanos, de manera que, al mismo tiempo que se realizaban los trabajos de ingeniería correspondientes, se han efectuado los análisis sociológicos, politológicos y jurídicos necesarios para determinar la viabilidad del sistema que se desarrollaba [13].

Con esta perspectiva metodológica, el desarrollo del proyecto se ha abordado mediante un equipo multidisciplinar, compuesto por investigadores pertenecientes tanto al campo de la ingeniería telemática como al campo sociopolítico: uno de ellos con sede en el Departamento de Ingeniería y Arquitecturas Telemáticas, DIATEL (Universidad Politécnica de Madrid) y el otro en el Departamento de Ciencia Política y de la Administración III (Universidad Complutense de Madrid).

2. Distintas aproximaciones al voto electrónico

Bajo la denominación de **voto electrónico** se engloban numerosas actuaciones que tienen en común el empleo de sistemas electrónicos en alguna fase del proceso electoral. El empleo de los ordenadores en estos procesos se remonta a 1964 cuando se utilizaron por primera vez en EEUU. Desde entonces su uso ha ido aumentando, permitiendo automatizar en mayor o menor medida el proceso de votación. Atendiendo al grado de automatización alcanzado podemos clasificar estas experiencias en distintos niveles.

En el **primer nivel** de esta clasificación está lo que podemos denominar el escenario “clásico” de votación. En este escenario se englobarían tanto las votaciones mediante papeletas, como aquellas que se sirven de tarjetas perforadas o de lectores ópticos. Estas experiencias no pueden ser consideradas como un sistema de voto electrónico propiamente dicho, pero hasta ahora, han sido un referente para los distintos escenarios electrónicos que se han propuesto.

En un **segundo nivel** se encontrarían los escenarios de votación que, basándose en la forma de operar del método clásico, sustituyen alguno de sus elementos físicos y procedimientos manuales por algún tipo de sistema o de proceso electrónico. Entre estos posibles escenarios tenemos aquellos que utilizan alguno o varios de los siguientes elementos: tarjetas magnéticas (para autenticar al votante o incluso para emitir el voto), urna electrónica (para la recepción y recuento de votos), pantalla (tablero) de votación (para seleccionar la opción de voto elegida), cabina electrónica (para garantizar la privacidad), software de distintos tipos (para el proceso de escrutinio). En todos estos escenarios, los procesos a automatizar son los que se realizan comúnmente en el colegio electoral. Estos procesos podemos sintetizarlos en tres: el primero es el de la autenticación del votante, el segundo es el proceso de votar propiamente dicho y el tercero, todo lo relativo a la gestión y procesado del contenido de la urna electoral. Todos los componentes electrónicos utilizados en estos escenarios, tratan de automatizar alguno de estos procesos.

Casi la totalidad de las actuaciones gubernamentales encaminadas a la automatización de los procesos de votación en los distintos países democráticos se encuadran en este nivel. Se han realizado experiencias de este tipo en Brasil, Bélgica, Holanda, Francia, Noruega, Dinamarca, Venezuela, Argentina, Costa Rica y Japón, entre otros. También en España se están desarrollando experiencias dentro de este escenario. En el País Vasco, a iniciativa de la Dirección General de Procesos Electorales del Departamento de Interior del Gobierno Vasco, se ha desarrollado un sistema de voto electrónico (Sistema Demotek [3]), basado en papeleta con lectura óptica. Aunque todavía no se ha empleado en ninguna elección gubernamental, ya se han realizado con éxito diversas pruebas piloto con este sistema.

Un **tercer nivel** en la clasificación de los escenarios de votación sería el de los que hacen uso de redes telemáticas. Aquí podríamos distinguir dos grupos: aquellos que utilizan las redes telemáticas (públicas o privadas) para la interconexión de los distintos colegios electorales, o bien

los que proponen la votación desde casa (normalmente a través de Internet). En los escenarios del primer grupo, el elector tiene que desplazarse hasta el colegio electoral (o centro equivalente de votación) para emitir su voto. Una vez allí, puede encontrarse con cualquier escenario de los que hemos considerado de segundo nivel. El uso de redes telemáticas para la interconexión de los colegios electorales y el organismo encargado de la supervisión final (con un papel equivalente al que en España desempeña la Junta Electoral Central) permite una rápida recolección de los datos y publicación de los resultados. El segundo grupo, votación desde casa a través de Internet, es el más atractivo, desde un punto de vista tecnológico, debido a los retos técnicos y de seguridad que plantea. Pero, a su vez, desde un punto de vista sociológico, plantea serios interrogantes debidos, en gran parte, a lo que puede conllevar que no todo el mundo tenga las mismas oportunidades de acceso. Recordemos que sufragio universal significa que las condiciones son las mismas para todos.

Dentro de este segundo grupo (**voto a través de Internet**) se han hecho también numerosos experimentos, la mayoría de los cuales han consistido en elecciones realizadas a pequeña escala y de baja importancia, en las cuales el fraude no implica grandes beneficios a los ganadores ni perjuicios de importancia a los perdedores. Habitualmente, estos sistemas no han cuidado el mantenimiento de las reglas casi universalmente aceptadas en las votaciones de gran escala, sobre todo en aquellas en las que se deciden gobiernos nacionales.

La propuesta de un Sistema de Votación a través de la red que llegue a tener aceptación por parte de los ciudadanos deberá, al menos, ofrecer las mismas garantías que nos brinda el sistema tradicional de voto, que además permite llevar a cabo un recuento visible de los votos, que puede ser revisado manualmente.

En el estado de California, el Secretario de Estado convocó a la *Internet Voting Task Force* para estudiar la posibilidad de emplear Internet para llevar a cabo las elecciones en California. Se reunieron expertos en el campo de seguridad, legislación y participación ciudadana y elaboraron un informe, publicado en enero del año 2000 [4]. Este informe recoge los requisitos de seguridad exigibles al nuevo sistema de votación y pone de relieve la necesidad de avanzar con cautela en el proceso de su introducción, ya que la posibilidad de amenazas o pirateo del sistema pondría en peligro el esfuerzo realizado. Sin embargo, afirma que, a pesar de los retos que supone el desarrollo del nuevo sistema, es técnicamente posible

utilizar Internet para desarrollar un método de votación, al menos tan seguro como los sistemas actuales. Asimismo, este informe propone el empleo de una estrategia *evolutiva* más que *revolucionaria* hacia el nuevo sistema, para su aceptación paulatina por los ciudadanos.

Como consecuencia de estos estudios, una experiencia muy interesante fue la realizada por la empresa Safevote entre el 30 de octubre y el 3 de noviembre de 2000 en el condado de **Contra Costa**, California, a través de Internet [2]. Esta prueba, encargada por la Secretaría de Estado de California, tenía como objetivo estudiar la viabilidad del voto por Internet ceñido a una circunscripción y determinar el nivel de aceptación del sistema de votación desarrollado por Safevote. Con esta prueba se pretendía, así mismo, detectar los posibles fallos en la seguridad de este sistema de votación. A **nivel europeo** se están realizando inversiones importantes para la puesta en marcha de sistemas de votación electrónica avanzados. Dentro del V Programa Marco de Tecnologías para la Sociedad de la Información se ha aprobado un proyecto (**CyberVote** [5]: septiembre 2000-marzo 2003), con el objetivo de desarrollar y demostrar el primer prototipo de CyberVote, utilizando las tecnologías móviles y fijas de Internet, que sea altamente seguro y verificable, diseñado para ser usado en elecciones locales, regionales, nacionales o europeas.

Otro proyecto, **E-Poll** [6] comenzó en el año 2000 y finalizará este año. El consorcio que desarrolla este proyecto está formado por empresas e instituciones de Alemania, Italia, Francia y Polonia. Este proyecto investiga las comunicaciones móviles de banda ancha basadas en el estándar UMTS para proporcionar a la red de E-Poll el ancho de banda y la seguridad requeridos.

3. Evaluación de propuestas de votación a través de redes telemáticas

De los sistemas comentados en el apartado anterior que tienen posibilidad de sustituir a los sistemas tradicionales, los que resultan interesantes son aquellos que incorporan mecanismos criptográficos para garantizar la seguridad en distintas etapas del proceso. Asimismo, es necesario que incluyan una adecuada política de seguridad que permita a los votantes supervisar el proceso.

Dentro del proyecto VOTESCRIPT se ha llevado a cabo un detenido estudio y evaluación de las propuestas más relevantes de votación a través de redes telemáticas que se apoyan, a su vez, en algoritmos criptográficos avanzados. A continuación se presenta un resumen simplificado de los esquemas más significativos.

Un hito importante en las propuestas de sistemas de Voto Electrónico fue la aparición en 1992 de *A Practical Secret Voting Scheme for Large Scale Elections*, propuesto por Fujioka, Okamoto y Ohta [7]. Esta propuesta define distintos agentes participantes en el proceso de votación y pone atención al cumplimiento de requisitos básicos del proceso electoral tradicional. También hace la aportación de ofrecer al votante la posibilidad de ejercer cierto grado de control del proceso. En 1995, Cranor [8] desarrolla un prototipo (denominado Sensus) llevando a la práctica, con algunas modificaciones, las ideas propuestas por Fujioka. Dos años más tarde Herschberg implementa otro prototipo (EVOX) [9] basado en las mismas líneas generales. En 1999 Fujioka y otros autores presentan *An Improvement on a Practical Secret Voting Scheme* [10] del que no tenemos constancia que exista alguna implementación.

En el entorno español, en 1999 Riera presenta en la Universidad Autónoma de Barcelona la Tesis Doctoral titulada *Design of Implementable Solutions for Large Scale Implementable Voting Schemes* [11] del que tampoco tenemos constancia de que exista alguna implementación.

A grandes rasgos, se podría resumir la propuesta inicial de **Fujioka, Okamoto y Ohta** de la siguiente forma. Existen tres componentes: votantes, un Administrador y un Contador. El votante solicita al Administrador la *firma a ciegas* o *firma opaca* de su voto cifrado con una clave particular para cada votante (firma a ciegas implica que el Administrador conoce la identidad de quien solicita la firma, pero no tiene posibilidad de conocer el contenido de lo que firma, por lo que no podrá conocer el contenido del voto, del cual se dice que está *opacado*).

El Administrador firmará solamente si el votante está entre los autorizados y no ha votado ya. El votante envía al contador el voto cifrado con su clave de votación (pero desopacado) y firmado por el Administrador. El Contador acepta el voto únicamente si está debidamente firmado por el Administrador. Finalizado el periodo de recepción de votos, tanto el Administrador como el Contador, publican sendas listas con información para ser verificadas y reclamadas por los votantes que detecten que su voto no está siendo considerado adecuadamente. Así, el Administrador publica una lista en la que aparece la identificación de cada uno de los votantes que han enviado su voto al administrador junto con el voto opacado y la firma del propio Administrador.

Por su parte, el Contador publica otra lista en la que aparece el voto cifrado con la clave del votante junto a la firma del Administrador y un número de identificación que el propio Contador le ha asignado. Cada votante

comprueba que su voto esté correctamente registrado y que la cantidad total de votos publicados por el Contador coincida con la lista publicada por el Administrador. Si todo es correcto, el votante envía al Contador la clave junto a su número de identificación (obtenido de la lista) que servirá para descifrar su propio voto.

Los autores de esta propuesta destacan que ni el Contador ni ningún otro agente, tiene posibilidad de conocer un avance del resultado de las elecciones antes que se haya cerrado la recepción de votos. Una vez descifrados todos los votos el Contador hace público el resultado final.

Las críticas a esta propuesta abarcan, por un lado, a lo que en ella se dice explícitamente y por otra parte a algunos elementos que no se explican con precisión. En la primera categoría se encuentra la diferencia fundamental con el método tradicional, ya que el votante debe tomar contacto con el sistema en dos ocasiones, separadas en el tiempo, pero dentro del periodo de votación: primeramente, obtiene la firma del Administrador y envía el voto al Contador, y posteriormente, cuando todos los votantes han realizado esta primera parte del proceso, accede por segunda vez al sistema para verificar que su voto haya sido recibido correctamente en el Contador y, en ese caso, enviar la clave para que el Contador pueda descifrarlo. Además, hace también suposiciones poco factibles en elecciones a gran escala como que ningún votante se abstiene o que el Administrador y el Contador son honestos.

En la segunda categoría, aquello que la propuesta no dice, cabe destacar que no indica la forma de abordar problemas tales como los derivados de fallos en la comunicación y por lo tanto de cómo distinguir si la información (votos o claves) no ha llegado al Contador por problemas técnicos o humanos, sean estos últimos intencionados o no. Desde este punto de vista, es previsible que existan dificultades en la atención de reclamaciones de votantes que después de solicitar la firma del Administrador no envíen el voto al Contador, o que habiendo realizado estos dos primeros pasos no realicen el tercero consistente en enviar la clave, o que envíen al Contador una pareja "numero de identificación y clave" incorrecta. También el sistema puede ganarse la desconfianza de los participantes en el proceso electoral ya que es absolutamente necesario que el Administrador y el Contador sean completamente honestos e independientes entre sí, puesto que de otra forma existiría riesgo de emisión de votos extras por parte de estos sistemas.

En lo referente a la implementación de **Sensus**, la información de que se dispone indica que ésta es una

adaptación del primer modelo propuesto por Fujioka de 1992, con alguna modificación, principalmente buscando la comodidad para el votante, evitándole ese doble contacto con el sistema. El precio de esta modificación es la de permitir al Contador el conocimiento de los resultados parciales, ya que en una sola sesión el votante obtiene la firma ciega de su voto por parte del Administrador, envía su voto cifrado (pero desopacado) al Contador, recibe el número de identificación y envía al Contador la clave para descifrar el voto. Con esto acaba la participación del votante en el proceso. No obstante, no se indica en la documentación ofrecida en la página web correspondiente cómo aborda los posibles problemas de comunicación y, por el contrario, se expresa que la implementación del canal anónimo queda fuera del ámbito de su desarrollo. Este canal anónimo es necesario para transmitir la información entre votante-Administrador y votante-Contador y viceversa.

EVOX es otra implementación de la propuesta de Fujioka, aunque incorpora modificaciones sustanciales, haciendo aparecer dos nuevos componentes: un Anonimizador y un Comisario. El Anonimizador se encarga de romper la relación existente entre el votante y el voto con el objeto de no pedirle al votante ese doble contacto con el sistema. El votante, obtiene la firma a ciegas del Administrador y envía al Anonimizador el voto oculto firmado, junto con el voto oculto sin firmar, la elección en claro y dos claves empleadas para formar el voto oculto. Esta comunicación hace uso de una conexión segura entre votante y Anonimizador que se apoya en otra existente entre votante y Contador. El uso doble de estos canales seguros protege al votante de forma que el Anonimizador no pueda conocer el contenido del voto mientras conozca la identidad del votante, en tanto que el Contador podrá conocer el contenido del voto pero no la identidad del votante. El Anonimizador y el Contador deben ser elementos completamente honestos e independientes para impedir que se pueda establecer relación entre el contenido del voto y la identidad del votante. El Comisario es un elemento encargado de supervisar el funcionamiento de todo el sistema.

La propuesta denominada *An Improvement on a Practical Secret Voting Scheme* presentada en 1999 por Fujioka y otros autores difiere de la anterior al incorporar un tablón de anuncios y un número n de contadores que han de colaborar entre sí para realizar el recuento, permitiendo que aunque alguno de los contadores se niegue a colaborar este recuento pueda proseguir. Para ello, usa un mecanismo de encriptación de umbral, esto es: el votante

cifra su voto sucesivamente n veces con n claves diferentes, de tal forma que sea suficiente una cantidad t de claves para descifrarlo, siendo t menor que n . El votante envía su voto cifrado con las claves de los contadores al tablón de anuncios de forma que todos puedan ver que el voto ha llegado pero éste no puede ser descifrado hasta que una cierta cantidad mínima, de al menos t contadores, se pongan de acuerdo para descifrarlo. Soluciona el inconveniente de la primera propuesta, en la cual todos los electores debían esperar al momento en que finalizara la recepción de votos para, a continuación, enviar la clave que permitiría descifrar el voto.

La propuesta realizada en la tesis doctoral de Andreu Riera, *Design of Implementable Solutions for Large Scale Implementable Voting Schemes* propone un sistema para la votación a gran escala, semejante a las que se pueden producir en unas elecciones generales a nivel nacional. Basa su funcionamiento en la distribución de los elementos que intervienen (votantes, colegios electorales, centros de recuento y una Autoridad de Elección) que se estructuran jerárquicamente en forma de árbol, lo que permite que el sistema sea escalable. En el nivel superior de la jerarquía se encuentra una Autoridad de Elección que, en la mayoría de las elecciones tradicionales, representa al organismo institucional que debe responsabilizarse de la organización y del buen funcionamiento de la votación. De esta Autoridad dependen directa o indirectamente los Centros de Recuento. En el nivel inferior de la jerarquía, y dependiendo de los Centros de Recuento se encuentran los Centros de Votación. Para obtener el anonimato del votante se utilizan Agentes Móviles que actúan en la fase de recuento, cuando ya todos los votos han sido emitidos, y se encargan de recoger y mezclar el contenido de la urna. Para prevenir la compra y venta masiva de votos propone la distribución a todos los votantes de tarjetas inteligentes inmodificables (*tamper-proof smartcards*).

En un punto de vista totalmente contrario a los anteriores se encuentran las críticas formulada por Mercuri [12], quien se declara "firmemente contraria al uso de sistemas completamente electrónicos o basados en Internet para que sean aplicados en la emisión del voto y en el recuento de los mismos". En el año 2001, ante el Comité de Ciencias de la Cámara de Representantes de los Estados Unidos, expuso una exhaustiva relación de razones para argumentar su posición, y planteó un grupo de preguntas que permiten valorar la seguridad de los sistemas de votación electrónica. Sus argumentos, aparte de los estrictamente relacionados con características locales, de interés para su audiencia, se podrían resumir en que ella

asegura que es imposible superar aspectos tan críticos como son el incremento desmesurado del riesgo de venta de votos, coacción, monitorización clandestina, denegación abusiva del derecho a voto y entrega de resultado finales oficiales distintos de los verdaderos. Indica que no hay forma de ofrecer al votante la seguridad de que el voto se ha registrado tal cual ha sido emitido, o que el recuento es el correcto; que no ofrece control por parte de los partidos políticos, que los defectos del sistema pueden ser conocidos años después de la elección, que no hay elementos de auditoría, que los mecanismos criptográficos se pueden romper tarde o temprano y que desde el mundo entero se pueden atacar los sistemas telemáticos. Los autores de esta ponencia están convencidos de que la propuesta elaborada dentro del proyecto VOTESCRIPT da respuesta mayoritariamente satisfactoria a estas objeciones.

4. Procesos multidisciplinarios para la determinación de los requisitos de usuario del sistema VOTESCRIPT

Como ya se indicaba en el apartado de Introducción, el desarrollo del sistema VOTESCRIPT se ha abordado desde una perspectiva multidisciplinar. En opinión de los autores, la multidisciplinaridad en las investigaciones llevadas a cabo por equipos conjuntos no debe ser la suma de trabajos realizados en compartimentos estancos, sino el aprovechamiento de la sinergia que aparece al abordar los temas desde las perspectivas (en nuestro caso) tecnológicas, sociopolíticas y jurídicas.

Consecuentemente con ello, el grupo de investigación abordó la tarea de determinar los requisitos de los sistemas de votación, con el objetivo de diseñar un sistema técnico que satisfaga las necesidades sociales de los ciudadanos y garantice los derechos democráticos jurídicamente existentes.

En este sentido, la investigación del grupo partió de una revisión de la literatura existente sobre este particular y llevó a cabo un análisis crítico de los requisitos detectados en los distintos sistemas de votación que habían sido propuestos con anterioridad.

En estos escritos sorprende el poco peso que, en general, se suele otorgar a los requisitos que deben cumplir los sistemas telemáticos de votación. Las siete condiciones para construir un esquema de votación segura planteados en 1992 por Fujioka [7] fueron las que sirvieron de base para posteriores diseños. A nivel internacional, una referencia recurrente en lo relativo a los requisitos de usuario para la votación electrónica la encontramos en los

propuestos por Cranor [8] y su protocolo Sensus, que en España han sido heredados en la propuesta elaborada por Riera en su tesis doctoral [11] antes citada. Una primera crítica al esquema de Cranor, radica en que el requisito de *privacidad* se define como que todo voto ha de permanecer secreto, es decir asimilando privacidad a anonimato y confidencialidad, dejando a un lado otros servicios de seguridad y condicionantes que son fundamentales para la consecución de la privacidad.

Llama la atención, por su simpleza, que el único requisito vinculado a temática social, sea el denominado *democracia* definido como: *solo las personas con derecho a voto, votan, y solo pueden hacerlo una vez*. Frente a esta definición se pueden plantear los casos de regímenes políticos con sistema de gobierno dictatorial que realizan votaciones que cumplen con estas condiciones, sin que ello implique, en ningún caso su conversión en sistemas democráticos (si no se tiene en cuenta el resultado de la votación no podemos hablar de democracia).

La democracia, sus condiciones y necesidades de funcionamiento, así como sus implicaciones para la organización de la ciudadanía, son temáticas difícilmente plasmables en tan pocas palabras. Teorizar sobre democracia digital requiere un esfuerzo y constancia intelectual en el que las trivializaciones son imperdonables. En su relación con la telemática, no es lo mismo un diseño técnico para una aplicación industrial, que un sistema que vertebró los derechos de los ciudadanos, tarea a todas luces bastante sensible y complicada.

La experiencia nos permite afirmar que el tener en cuenta los requisitos y las demandas del ámbito sociopolítico conlleva un perfeccionamiento técnico de los sistemas desarrollados, en comparación con aquellos otros que, trabajando exclusivamente con la perspectiva telemática, diseñan los sistemas por sí mismos, aplicando como herramientas de reflexión sociológica, la que buenamente pueda proveer su inteligencia y capacidad de reflexión.

El proceso de trabajo llevado a cabo por nuestro grupo fue el siguiente:

El primer análisis de la literatura y los requisitos que se manejaban a nivel internacional mostró que eran muy insuficientes, tanto en los aspectos técnicos como en los sociológicos. En el documento de Contra Costa [2] la lista de requisitos que seleccionan es más extensa y detallada que en los casos antes comentados pero, tal y como están formulados, parecen más una relación de características y bonanzas del sistema desarrollado que un conjunto de necesidades que el sistema debería cumplir. Más interés

para el grupo de trabajo tuvieron las recomendaciones contenidas en el informe del Internet Policy Institute[1].

A partir de esta literatura y su análisis técnico el equipo multidisciplinar elaboró un nuevo conjunto de requisitos mediante un amplio proceso de discusión. Una vez definidos, se realizó una investigación de campo sociológica de carácter cualitativo para determinar, de forma genérica las actitudes de los ciudadanos ante la utilización de sistemas telemáticos para la votación electrónica y evaluar la aceptación y utilidad de los requisitos.

Frente a las técnicas de investigación cuantitativas (la más conocida sería la encuesta), en la investigación cualitativa se busca la genealogía de los discursos esgrimidos por los investigados¹. Una vez concluida esta fase, se incorporaron los análisis e informaciones extraídas de esta investigación y se elaboró el conjunto de requisitos que a continuación se presenta. Cabe señalar que algunos de estos requisitos fueron en principio detectados más bien como procedimentales, pero a la luz de la investigación social, aparecen como garantes del sistema de votación al satisfacer demandas que surgen con fuerza en los trabajos de campo realizados. Por ejemplo, la necesidad de tener una garantía individual (“recibo”) de lo que se ha votado para evitar actuaciones fraudulentas.

Obviamente, dichos requisitos no se establecen como definitivos, sino que están sometidos a posibles modificaciones, incorporaciones o exclusiones en función de las investigaciones multidisciplinarias que se sigan desarrollando. Es un proceso que permanece abierto a la constante interacción de las sugerencias técnicas, politológicas, jurídicas y sociológicas, y en el momento de escribir este texto, los requisitos se encuentran de nuevo sometidos a evaluación mediante otra investigación sociológica en la que se tiene presente el modelo de votación propuesto en VOTESCRIPT.

Pasemos a exponer los requisitos detectados hasta ahora:

4.1. *Autenticidad* o *Autenticación*: sólo los votantes autorizados pueden votar.

4.2. *Acotabilidad* o *Singularidad (Uniqueness)*: el sistema tan solo autentica la votación dentro de las

reglas establecidas. Es decir, por regla general, cada votante sólo puede votar una vez.

4.3. *Anonimato*: no se puede relacionar un voto con el votante que lo ha emitido. Dentro del anonimato pueden distinguirse dos aspectos.

- Mecanismos que eviten que los agentes telemáticos presentes en el sistema puedan coludir.
- Posible extensión del anonimato al ejercicio de la abstención.

4.4. *Imposibilidad de coacción*: ningún votante debe ser capaz de demostrar ante terceros qué voto ha emitido.

4.5. *Verificabilidad individual*: cada votante deberá poder asegurarse de que su voto ha sido considerado adecuadamente, de forma que pueda obtener una prueba palpable de este hecho. Podemos distinguir dos tipos de verificabilidad individual:

- Verificabilidad individual del contenido del voto emitido.
- Verificabilidad individual de que el voto ha sido tenido en cuenta adecuadamente.

Definida de esta forma, la verificabilidad individual puede aparecer una cierta contradicción con el requisito de imposibilidad de coacción. Cuanto más explícita es la verificación individual más riesgos de coacción pueden aparecer. No obstante, se pueden diseñar mecanismos no exclusivamente telemáticos, que hagan compatibles ambos requisitos. En el sistema convencional, el votante sabe lo que vota, y confía en que su voto será contabilizado correctamente cuando comprueba que es introducido en la urna (verificabilidad individual). Además, si usa una cabina para cumplimentar su voto, no hay peligro evidente de coacción. Como puede intuirse, un estudio mínimamente riguroso del balance entre los requisitos de verificabilidad y coacción requeriría la inclusión y análisis de más parámetros, dependiendo de los distintos condicionantes sociales que aparecen en cada situación concreta.

Se vislumbran dos posibles soluciones de cara a equilibrar la relación entre verificabilidad individual e imposibilidad de coacción:

- Temporalidad de la validez de la verificabilidad individual. Se limita en el tiempo la posibilidad

¹ En la investigación sociológica cualitativa se trata de captar lo generativo, las ideas-fuerza, los textos que se encuentran en la base de la producción del discurso. En las técnicas cualitativas el sujeto investigado se encuentra *libre* para decir aquello que le plazca sobre la temática discutida. Así se puede extraer información relevante que difícilmente puede aparecer en un ámbito tan restrictivo como es la encuesta.

de la verificabilidad individual. Pasado dicho tiempo se destruyen los ficheros.

- La verificabilidad individual se puede ejercer a través de mecanismos mixtos, no exclusivamente telemáticos.

4.6. *Verificabilidad Global*. Otra forma mediante la cual el votante puede asegurarse de que su voto ha sido considerado adecuadamente es que dentro del propio sistema existan mecanismos que permitan a los ciudadanos autorizados comprobar la validez del recuento final.

4.7. *Fiabilidad*: El sistema debe de garantizar que no se produce ninguna alteración de los resultados, ya sea mediante ataques intencionados, fallos en el sistema o incluso si las Autoridades del sistema se ponen de acuerdo para coludir.

- Fiabilidad en los procedimientos (*Reliability*). El sistema debe trabajar de forma robusta, incluso en el caso de numerosos fallos, incluyendo fallos masivos en las máquinas de votación o pérdida total de las comunicaciones.
- Exactitud en el recuento (*Accuracy*): El sistema debe registrar correctamente todos los votos. Todos los votos son tenidos en cuenta sin que sea posible cambiar, borrar o extraviar ningún voto. El sistema ha de proporcionar 100% de exactitud.
- Integridad de los datos (*Data Integrity*). Se garantiza que el contenido del voto u opinión es exactamente el que fue enviado, de tal forma que al texto original no le ha sido añadida, ni modificada, ni sustraída alguna de sus partes.

4.8. *Certificabilidad o Auditabilidad*: durante el proceso de votación deberían registrarse las pruebas de voto y elementos de auditoría que permitieran a las personas autorizadas disponer de pruebas para comprobar que todo el proceso de votación es correcto (funcionamiento del sistema, programas, equipos, protocolos y demás elementos), todo ello sin comprometer la integridad de la elección o la privacidad y anonimato de los votantes. Se pueden distinguir dos tipos de auditabilidad:

- Auditabilidad al desarrollo y ejecución del sistema durante el proceso de votación.
- La Auditoria y obtención de pruebas sobre la votación han de permitir que sea físicamente almacenable, recuperable y comparables *off-line*. Este requisito se puede considerar en sus

objetivos coincidente con el requisito 4.6 *verificabilidad global*.

4.9. *Neutralidad*: no debe ser posible conocer resultados parciales hasta que no finalice el tiempo de la elección.

4.10. *Movilidad de los votantes*. El sistema debería permitir a los participantes que emitieran su opinión o voto desde cualquier *cabina o punto de votación*, eliminando la restricción actual de hacerlo en el centro de votación de la zona en la cual está censado.

4.11. *Facilidad de uso*. El votante debe necesitar el mínimo de habilidades y conocimientos especiales para emitir el voto.

4.12. *Voto rápido*. El votante debería poder emitir el voto en un tiempo mínimo y razonable.

4.13. *Voto nulo o de rechazo*. Posibilidad de emitir un voto sin que sea contabilizado como válido para ninguna de las candidaturas propuestas ni ser considerado dentro del bloque de los votos en blanco.

4.14. *Código abierto*: el código fuente de todos los programas debería de ser conocido y verificable por los auditores. La seguridad del sistema no debería estar basada en mantener este código secreto, sino en las claves de cifrado utilizadas en todas las fases del proceso de votación. Además, para garantizar su carácter abierto en futuras aplicaciones, el modelo de licencia propuesto para este software es del tipo comúnmente denominado *copyleft*.

4.15. *Coste mínimo*. El coste del sistema de elección debería de ser abordable y en consonancia con el coste del sistema convencional.

4.16. *Utilización de una red dedicada*. Tanto si se vota a través de Internet como si se vota desde cabina especializada, la red telemática en la que se apoya el sistema deberá ser, desde un punto de vista lógico, totalmente cerrada, de forma que el acceso a ella sólo esté permitido a los agentes y actores contemplados en el sistema.

4.17. *Compatibilidad con otros mecanismos de votación convencionales*. Poder elegir entre el sistema tradicional de urna (o voto por correo) y el sistema de votación electrónica.

4.18. *Igualdad de oportunidades en la votación*. Todo ciudadano ha de tener acceso al equipamiento técnico y procedimientos organizativos a la hora de votar.

El acceso desde casa, quizás a través de Internet, plantea innumerables ventajas, pero, en la situación actual, conlleva unos riesgos capitales en lo relativo a lo que en sociología se conoce como Estratificación Digital. Se entiende por *Estratificación Digital* (en inglés *Digital Divide*) los trabajos que abarcan el estudio de los discursos y prácticas asociadas con las desigualdades y diferencias en el acceso a computadores, infraestructura de entrada a la red y adquisición de conocimientos, que se dan entre las distintas clases sociales, así como por etnia, género, nivel educativo, convicciones políticas o religiosas, etc..

Esta preocupación por las desigualdades ha sido fuertemente detectada en los trabajos de campo llevados a cabo. Un sistema de Democracia Digital necesariamente conlleva el derecho de acceso del conjunto de la ciudadanía: sería una proyección telemática del concepto de Sufragio Universal.

- 4.20. *Flexibilidad Física*. El equipamiento debe de poder ser usado por gente con alguna discapacidad física.
- 4.21. *Digno de confianza*. El votante debería entender el proceso de votación para fortalecer su confianza en el sistema.

5. Visión global del Sistema de Votación diseñado

Se presenta a continuación la definición de los servicios de seguridad que deberá proporcionar el sistema de votación que se propone dentro del proyecto VOTESCRIPT, las autoridades o agentes necesarios para realizar el proceso seguro de votación, las relaciones entre los distintos componentes del sistema de voto, las credenciales necesarias y el procedimiento propuesto.

5.1. Consideraciones previas

Como paso previo al comienzo de la votación, se habrá hecho llegar a los votantes una tarjeta inteligente y un identificador de votante que deberá ser conocido por todos los miembros de la elección.

La tarjeta inteligente, diseñada especialmente para este proyecto, es capaz tanto de generar claves como de realizar gran parte de los procesos criptográficos necesarios para la seguridad del sistema. Implementa para ello diversos

algoritmos adicionales, además de los ya habituales en las tarjetas inteligentes.

Para llevar a cabo este diseño, se ha optado por un sistema en el que el votante debe de utilizar una cabina de votación, en vez del voto desde casa por Internet. De esta forma, se pretende satisfacer de forma más adecuada los requisitos de seguridad necesarios, así como la problemática de la compra de votos, la coacción en el momento de la emisión del voto y la posibilidad de ligar el voto con la ubicación física del votante. Se deja para una fase posterior, tal y como se comenta en el apartado de Introducción, la adaptación de este sistema para el voto por Internet. No obstante, este grupo de investigación también está colaborando con la FNMT-RCM en la implantación de un sistema de voto por Internet para un conjunto reducido de votantes.

5.2. Arquitectura del sistema

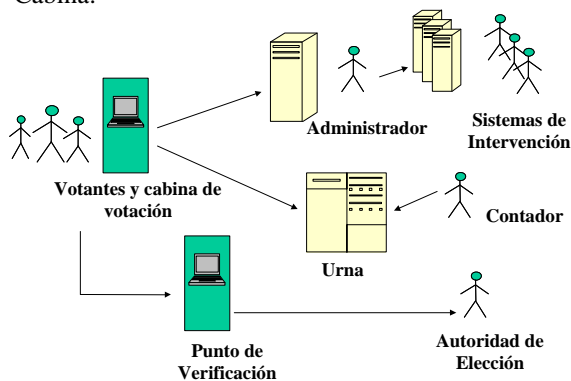
El escenario se compone de un conjunto de sistemas automáticos: las Cabinas de Votación, un Administrador o autoridad de identificación, un Sistema de Intervención por cada una de las distintas candidaturas que se determine deban participar en la fase de votación, una Urna, un proceso Contador y un conjunto de Puntos de Verificación. El sistema contempla, además, la existencia de una autoridad (persona jurídica) encargada del control general que se ocupa de atender todas aquellas posibles reclamaciones con respecto al funcionamiento del sistema. A esta autoridad se le ha asignado el nombre de *Autoridad de Elección* y su funcionalidad se describe más adelante.

La funcionalidad de cada uno de ellos es la siguiente:

- *Cabina de Votación*: Se considera Cabina de Votación al conjunto formado por el software cliente instalado en la cabina y la tarjeta inteligente de la persona que quiere entregar su voto. Su funcionalidad principal es la de interactuar con los demás agentes del sistema, concretamente con el Administrador y la Urna, dándole a la elección del votante el formato adecuado para cada interacción. Permite a la persona que quiere votar entregar su voto de forma segura.
- *Administrador*: El Administrador es la entidad encargada de validar la clave de un votante durante la elección. Se encarga de comprobar si el identificador del votante que solicita la validación de su clave tiene el formato correcto, si el votante asociado a dicho identificador está autorizado a votar y si no se le ha validado ya una clave, validándosele en caso de que se cumpla con todo lo anterior. Se encarga también de

hacer llegar la solicitud de validación de clave a cada uno de los Sistemas de Intervención y de recoger la respuesta de estos y enviársela a la Cabina.

- **Sistemas de Intervención:** Al igual que ocurría con el Administrador, la función de cada uno de los Sistemas de Intervención es la de validar la clave de votación de un votante. Cada Sistema de Intervención recibe del Administrador la solicitud de validación enviada por un votante, comprueba si el identificador de votante tiene el formato correcto, si el votante está autorizado a votar y si se le ha validado con anterioridad una clave, validándosele en el caso de que no haya sido así y se cumpla todo lo anterior. Ante la solicitud de validación, cada Sistema de Intervención devuelve su respuesta al Administrador, que se encargará de hacerla llegar a la Cabina.



Cada uno de los Sistemas de Intervención está controlado por un interventor. Estos sistemas, que forman parte del sistema global, serán proporcionados por la Administración Pública y no serán elementos propiedad de las candidaturas. Se prevé que estén ubicados en el mismo entorno que el Administrador y que sus programas estén homologados y sean resistentes ante ataques. Asimismo, se prevé que pueden ser auditados por peritos de confianza de las candidaturas antes del proceso de votación.

La existencia de los Sistemas de Intervención es una de las principales aportaciones de esta propuesta, puesto que permite el control, por parte de los partidos políticos, de todo el proceso electoral, a la vez que les dota de la posibilidad de realizar de forma sencilla una auditoría no sólo del resultado final sino de todo el proceso.

- **Urna:** La Urna es la entidad encargada de recoger y almacenar los votos entregados por cada votante hasta

el final del periodo habilitado para la entrega. Además de recoger y almacenar el voto, genera y envía a la Cabina un comprobante de su entrega, que ésta guarda en la tarjeta inteligente del votante, con el que posteriormente el votante podrá reclamar en el caso de que detecte un tratamiento incorrecto de su voto por parte del sistema.

- **Contador:** La funcionalidad principal del Contador es la de realizar el recuento de los votos. Una vez finalizado el proceso de entrega, los votos almacenados en la Urna son entregados al Contador, que se encarga de descifrarlos, comprobar que se trata de votos válidos y contarlos, publicando posteriormente las listas finales de resultados.
- **Puntos de Verificación:** Los puntos de verificación son elementos cuya funcionalidad es la de proporcionar a los votantes un lugar en el que llevar a cabo la verificación individual del tratamiento dado a su voto por parte del sistema. Mediante la verificación individual cada votante podrá comprobar, de forma independiente, si su voto se ha tenido en cuenta y ha sido correctamente contabilizado. Estos puntos de verificación pueden ser las mismas cabinas de votación u otros sistemas adicionales. El principal requisito de seguridad que se les exige es que no den publicidad a la clave con que se ha emitido el voto para evitar así la compra de votos.
- **Autoridad de Elección:** La Autoridad de Elección es la encargada del control general del sistema, de velar por su correcto funcionamiento, ocupándose de atender todas aquellas posibles reclamaciones que realicen los votantes. En el caso de que se produzca una reclamación por parte de un votante sobre el tratamiento dado a su voto, ésta descubrirá y comparará todas las pruebas criptográficas presentes en el sistema para comprobar la validez del recuento. Solicitará al votante la tarjeta utilizada para la votación y, a partir de ella, podrá demostrar sin ninguna ambigüedad un tratamiento correcto o incorrecto del voto apoyándose en pruebas criptográficas robustas. Podrá determinar si el votante tiene o no razón, si ha existido o no una falsificación por parte del sistema, y estará en condiciones de llevar a cabo las acciones necesarias en cada caso.

En los trabajos de VOTESCRIPT no se ha abordado el proceso de registro de votantes y de la adecuada distribución de las tarjetas inteligentes así como el proceso mediante el cual al Administrador y los Sistemas de

Intervención se les proporciona, antes de la elección, una lista de identificadores de votantes autorizados y sus claves públicas, que permitirán comprobar si un votante que solicita participar en el proceso de votación está o no autorizado a votar.

5.3. Procedimiento de Verificación

Verificación individual

La verificación individual podrá ser realizada por los votantes a través de los Puntos de Verificación, una vez finalizado el proceso de votación y durante un tiempo limitado. El votante que desee verificar su voto acudirá a uno de estos Puntos de Verificación y previa identificación se le permitirá acceder, de forma individual, a un sistema en el que introduciendo la tarjeta inteligente, podrá leer en una pantalla el voto que a él le ha sido contabilizado por el Contador, no entregándosele ninguna prueba de esta comprobación. Caso que el votante crea que votó por una opción distinta a aquella que le ha sido mostrada podrá iniciar un proceso de reclamación, entregando su tarjeta inteligente a la Autoridad de Elección, la cual descubrirá y comparará todas las pruebas criptográficas presentes en el sistema para comprobar la validez del recuento.

La Autoridad de Elección podrá tomar las medidas que considere oportunas pudiendo llegar éstas incluso a la anulación del proceso de votación.

Con todo ello la Autoridad de Elección, apoyándose en pruebas criptográficas robustas, podrá dictaminar si el votante no tiene razón o si ha existido una falsificación por parte del sistema.

Verificación global

Una vez publicados los resultados de la votación, y con la intención de que las distintas candidaturas obtengan una prueba del correcto funcionamiento del Contador a la hora de abrir y contar votos, se permite que cada una de ellas verifique el procedimiento. Para ello, cada candidatura tiene la posibilidad, mediante una serie de procedimientos concretos que se han diseñado, de comparar la información que posee con la que se ha obtenido como resultado final del proceso de recuento. Caso de que ambas informaciones no se correspondieran, podrían proceder a impugnar la votación, presentando para ello pruebas criptográficas robustas.

Esta posibilidad de descubrir el fraude (cualquier ciudadano o cualquier partido político puede fácilmente descubrirlo), aleja la tentación de realizarlo.

5.4. Proceso genérico

A continuación, se resumen los pasos más relevantes del proceso propuesto para llevar a cabo una votación electrónica:

1. El votante, dentro de la cabina de votación, y después de autenticarse frente a su tarjeta inteligente, interactuará con el software de la Cabina, el cual genera en la tarjeta el par de claves que se emplearán para votar, opaca para el Administrador y cada uno de los Sistemas de Intervención la clave que utilizará para el descifrado y la envía junto con el identificador de votante al Administrador, todo ello cifrado de manera que sólo este último pueda leerlo.
2. El Administrador comprueba si lo recibido de la Cabina es correcto y si es así, reenvía el identificador de votante y la clave de descifrado opacada a cada uno de los distintos Sistemas de Intervención.
3. Cada uno de los Sistemas de Intervención, tras comprobar la validez del identificador de votante, firma de forma ciega la clave de descifrado opacada y se la devuelve al Administrador.
4. El Administrador firma de forma ciega la clave de descifrado opacada y se la devuelve a la Cabina junto con las recibidas de cada uno de los Sistemas de Intervención, todo ello cifrado de manera que sólo la Cabina pueda leerlo.
Hay que resaltar aquí que las claves de cifrado y descifrado residen en la tarjeta inteligente y que el votante no tiene posibilidad de leerlas.
5. La Cabina, apoyándose en las funcionalidades de la tarjeta, elimina el factor de opacidad y comprueba todas las firmas de la clave de descifrado. Si todo es correcto cifra su voto con la clave de cifrado y lo envía a la Urna junto con las firmas de la clave de descifrado a través de un canal seguro Cabina-Urna que se apoya en otro entre Cabina y Contador.
6. La Urna elimina el canal seguro Cabina-Urna y almacena la información recibida hasta el final de periodo de votación. Además de almacenar dicha información, forma con ella un comprobante de entrega de voto cifrándola con su clave secreta y posteriormente con la clave pública de la Autoridad de Elección. Una vez hecho esto, devuelve de manera segura dicho comprobante a la Cabina. Ésta, tras eliminar el canal seguro, almacena el comprobante en su tarjeta inteligente de manera que sólo la Autoridad de elección podrá obtenerlo.

7. Una vez finalizada la elección se *abre* la Urna y se le proporciona al Contador su contenido y la clave necesaria para descifrarlo. Haciendo uso de dicha clave el Contador llevará a cabo el recuento de votos y la publicación de las listas con los resultados finales de la votación.

5.5. Garantías de seguridad

El sistema propuesto da cobertura técnica a los requisitos de usuario detectados por el equipo multidisciplinar del proyecto y revisado después del análisis sociológico.

Además, la implantación de este sistema parte del supuesto de que los programas que corran en los distintos agentes telemáticos serán publicados para común conocimiento de los electores y de las candidaturas. La instalación de ese software en las máquinas será auditable y los programas instalados no podrán ser modificados maliciosamente por parte de nadie, debido a que:

- Los programas de los servidores estarán contenidos en unidades de memoria resistentes ante ataques (*tamperproof*).
- El programa que corra en la Cabina de votación será proporcionado dinámicamente por el servidor correspondiente y estará firmado y protegido contra alteraciones de su contenido.

No obstante lo anterior, hay que destacar que la fortaleza del sistema se basa en la obtención, por parte de los distintos actores del sistema, de piezas de información criptográficamente robustas y seguras que podrán presentar como prueba ante terceros en caso de litigio o disconformidad con los resultados del proceso.

6. Conclusiones y trabajos futuros

Las soluciones técnicas que se adopten a la hora de diseñar un sistema de votación tienen un impacto social muy relevante en lo tocante al mantenimiento y mejora de los derechos y libertades de los ciudadanos y, consecuentemente, en el desarrollo de la democracia en la Sociedad de la Información.

Por todo ello, para el diseño del sistema se ha partido de un análisis crítico y exhaustivo de las experiencias y propuestas que habían sido formuladas con anterioridad y se ha optado por una metodología multidisciplinar (tecnológica, sociopolítica y jurídica) tanto para la determinación de los requisitos y condicionantes como para la evaluación del sistema final que se desarrolle.

En los apartados precedentes se ha expuesto un resumen de los trabajos desarrollados, por ahora, dentro del proyecto VOTESCRIPT. Hasta este momento, ya se ha conseguido definir y especificar el conjunto completo de protocolos que regulan la comunicación entre todos los agentes y actores que intervienen en el escenario de comunicación del sistema. Por razones de espacio y de oportunidad, se ha optado por describir en la presente ponencia solamente un resumen somero del comportamiento global del sistema.

En la actualidad se está en la fase de desarrollo e implementación de un prototipo con el que se espera realizar pruebas que permitan evaluar su validez tanto desde el punto de vista tecnológico (analizando la robustez y seguridad de los algoritmos y protocolos utilizados) como desde el punto de vista de su aceptación por los ciudadanos.

7. Referencias

- [1] Internet Policy Institute. *Report of the National Workshop on Internet Voting*, marzo 2001. <http://www.internetpolicy.org/research/results.html> (último acceso julio 2002).
- [2] Safevote. *Contra Costa County Internet Voting Report*, septiembre 2000. <http://www.safevote.com> (último acceso julio 2002).
- [3] Gobierno Vasco. *Elecciones en Euskadi*. <http://www1.euskadi.net/botoelek> (último acceso julio 2002).
- [4] California Internet Voting Task Force. *A Report on the Feasibility of Internet Voting*, enero 2002. http://www.ss.ca.gov/executive/ivote/final_report.htm (último acceso julio 2002).
- [5] CyberVote. *Notas de prensa*. <http://www.eucybervote.org> (último acceso julio 2002).
- [6] E-Poll. *Electronic polling system for remote voting operations*. <http://www.e-poll-project.net/E-Poll.pdf> (último acceso julio 2002).
- [7] Fujioka, T. Okamoto, K. Otha. *A Practical Secret Voting Scheme for Large Scale Elections*, Advances in Cryptology, AUSCRYPT'92, Lecture Notes in Computer Science 718. Springer-Verlag, Berlin, pp.244-251 (1993).
- [8] Cranor Lorrie F. y Cytron, Ronald K. *Design and Implementation of a Practical Security-Conscious Electronic Polling System*, WUCS-96-02, Departamento de Informática, Universidad de Washington, St. Louis, enero 1996.

- [9] Herschberg, Mark A. *Secure Electronic Voting Over the World Wide Web*, Tesis doctoral en Ingeniería Eléctrica e Informática, Massachusetts Institute of Technology, 1997.
- [10] M.Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto. *An Improvement on a Practical Secret Voting Scheme*. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlín, pp. 225-234, 1999.
- [11] Riera i Jorba, Andreu. *Design of Implementable Solutions for Large Scale Implementable Voting Schemes*, Tesis doctoral Universidad Autónoma de Barcelona, 1999.
- [12] Mercuri R. *Testimony presented to the U.S. House of Representatives Committee on Science*, Mayo 2001. <http://www.house.gov/science/full/may22/mercuri.htm> (último acceso julio 2002).
- [13] Carracedo J. y Carracedo J.D. *Telemática y sociología. Apuntes para una investigación mutlidisciplinar: tarjetas de crédito anónimas y democracia electrónica*. I Congreso Iberoamericano de Telemática. Cartagena, Colombia, 2001.